Microprocessor system for safety-critical control systems

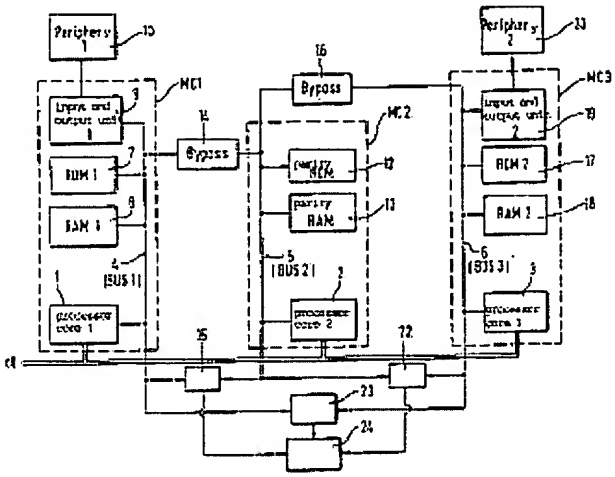
Patent number: DE19716197
Publication date: 1998-10-22
Inventor: GIERS BERNHARD (DE)
Applicant: ITT MFG ENTERPRISES INC (US)
Classification:
- international: ***B60G17/0185; B60T8/88; G05B9/03;*** **B60G17/015; B60T8/88; G05B9/03;** (IPC1-7): G06F11/14; B60G17/00; B60K28/16; B60T8/32; G05B9/03
- european: B60G17/0185; B60K41/28E; B60T8/88B; G05B9/03
Application number: DE19971016197 19970418
Priority number(s): DE19971016197 19970418

Also published as:
WO9848326 (A1)
EP0976012 (A1)
US6823251 (B1)
EP0976012 (B1)

Report a data error here

Abstract of **DE19716197**

The invention relates to a microprocessor system for safety-critical control systems. The inventive microprocessor system is equipped with at least three central units (1, 2, 3). Said units are arranged preferably on a single chip and run the same program. Read-only memories (7, 17) and read-write memories (8, 18) with additional storage locations (12, 13) for test data, input- and output units (9, 19), and comparators (15, 22, 23) are also provided. Said comparators check the output signals from the central units (1, 2, 3) to make sure that they agree. The central units (1, 2, 3) are interconnected via bus systems (4, 5, 6) and bypasses (14, 16). These bypasses enable the central units (1,2,3) to read and run the same existing data, including the test data and commands, according to the same program. The central units (1, 2, 3) are extended into two complete control signal circuits by means of redundant peripheral components (10, 20) and are connected with each other in such a way that if a breakdown occurs, the defective central unit (1,2,3) is identified and an emergency operation function is maintained, by majority decision.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 16 197 A 1**

(51) Int. Cl.[6]:
G 06 F 11/14
B 60 G 17/00
B 60 K 28/16
B 60 T 8/32
G 05 B 9/03

(21) Aktenzeichen: 197 16 197.9
(22) Anmeldetag: 18. 4. 97
(43) Offenlegungstag: 22. 10. 98

DE 197 16 197 A 1

(71) Anmelder:
ITT Mfg. Enterprises, Inc., Wilmington, Del., US

(74) Vertreter:
Blum, K., Dipl.-Ing., Pat.-Ass., 65779 Kelkheim

(72) Erfinder:
Giers, Bernhard, 60320 Frankfurt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

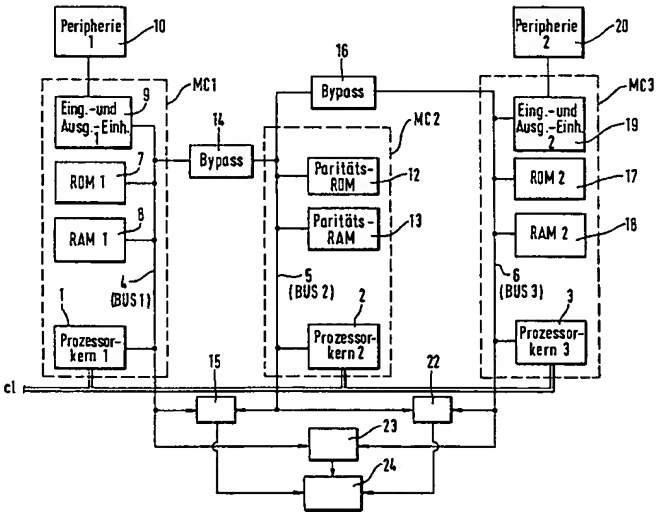
DE 41 36 338 C2
DE 41 22 016 C2
DE 30 24 370 C2
DE 195 29 434 A1
DE 195 09 150 A1
DE 44 39 060 A1
DE 43 41 082 A1
DE 41 37 124 A1
DE 38 25 280 A1
DE 35 33 849 A1
DE 32 25 455 A1

NIKOLAIZIK,Jürgen,NIKOLOV,Boris,WARLITZ,Joachim:
Fehlertolerante Mikrocomputersysteme, Verlag Technik GmbH, Berlin, 1990, S.80-84;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Mikroprozessorsystem für sicherheitskritische Regelungen

(57) Ein Mikroprozessorsystem für sicherheitskritische Regelungen ist mit mindestens drei, vorzugsweise gemeinsam auf einem Chip angeordneten Zentraleinheiten (1, 2, 3) ausgerüstet, die das gleiche Programm abarbeiten. Außerdem sind Festwertspeicher (7, 17) und Schreib-Lese-Speicher (8, 18) mit zusätzlichen Speicherplätzen (12, 13) für Prüfdaten, Eingabe- und Ausgabeeinheiten (9, 19) und Vergleicher (15, 22, 23) vorhanden, die die Ausgangssignale der Zentraleinheiten (1, 2, 3) auf Übereinstimmung überprüfen. Die Zentraleinheiten (1, 2, 3) sind über Bus-Systeme (4, 5, 6) und über Bypässe (14, 16) untereinander verbunden, die den Zentraleinheiten (1, 2, 3) ein gemeinsames Lesen und Abarbeiten der anstehenden Daten, einschließlich der Prüfdaten und Befehle, nach dem gleichen Programm ermöglichen.
Die Zentraleinheiten (1, 2, 3) sind durch redundante Peripherie-Komponenten (10, 20) zu zwei vollständigen Regelungssignalkreisen erweitert und derart zusammengeschaltet, daß bei einem Ausfall durch Majoritätsentscheid die fehlerhafte Zentraleinheit (1, 2, 3) identifiziert und eine Notlauffunktion aufrechterhalten wird.



DE 197 16 197 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Mikroprozessorsystem der im Oberbegriff des Hauptanspruchs beschriebenen Art. Es handelt sich also um ein System für sicherheitskritische Regelungen, mit redundanter Datenverarbeitung, mit mehreren Zentraleinheiten, welche über separate Bus-Systeme mit Festwertspeichern und Schreib-Lesespeichern, die auch Speicherplätze für Prüfdaten enthalten, mit Eingabe- und Ausgabeeinheiten und mit Vergleichern, die die Ausgangsdaten oder Ausgangssignale der Zentraleinheiten auf Übereinstimmung überprüfen, verbunden sind. Diese Zentraleinheiten arbeiten das gleiche Programm ab, wobei die Zentraleinheiten über die Bus-Systeme miteinander kommunizieren und wobei die Bus-Systeme untereinander durch Bypässe verbunden sind, die den Zentraleinheiten ein gemeinsames Lesen und Abarbeiten der anstehenden Daten, einschließlich der Prüfdaten und Befehle, ermöglichen.

Zu den sicherheitskritischen Regelungen dieser Art zählen u. a. die in die Bremsenfunktion eines Kraftfahrzeugs eingreifenden Regelungssysteme, die in großer Anzahl und großer Vielfalt auf dem Markt sind. Beispiele hierfür sind die Antiblockiersysteme (ABS), Antriebsschlupfregelungssysteme (ASR), Fahrstabilitätsregelungen (FDR, ASMS), Fahrwerksregelungssysteme etc. Ein Ausfall eines solchen Regelungssystems führt zur Gefährdung der Fahrstabilität des Fahrzeugs. Daher wird die Funktionsfähigkeit der Systeme ständig überwacht, um beim Auftreten eines Fehlers die Regelung abschalten oder in einen für die Sicherheit weniger gefährlichen Zustand umschalten zu können.

Noch kritischer sind Bremssysteme bzw. Kraftfahrzeug-Regelungssysteme, bei denen bei Ausfall der Elektronik keine Umschaltung auf ein mechanisches oder hydraulisches System möglich ist. Hierzu zählen Bremssystemkonzepte, wie "brakeby-wire", die voraussichtlich in der Zukunft noch an Bedeutung gewinnen werden; die Bremsenfunktion ist bei solchen Systemen auf eine intakte Elektronik angewiesen.

Ein Beispiel für eine Schaltungsanordnung oder ein Microprozessorsystem zur Steuerung und Überwachung einer blockiergeschützten Fahrzeugbremsanlage ist aus der DE 32 34 637 C2 bekannt. Nach dieser Schrift werden die Eingangsdaten zwei identisch programmierten Microcomputern parallel zugeführt und dort synchron verarbeitet. Die Ausgangssignale und Zwischensignale der beiden Microcomputern werden mit Hilfe von redundanten Vergleichern auf Übereinstimmung geprüft. Wenn die Signale voneinander abweichen, wird über eine ebenfalls redundant ausgelegte Schaltung eine Abschaltung der Regelung herbeigeführt. Bei dieser bekannten Schaltung dient einer der beiden Microcomputer zur Erzeugung der Bremsdrucksteuersignale, der andere zur Bildung der Prüfsignale. Bei diesem symmetrisch aufgebauten Microprozessorsystem sind also zwei vollständige Microcomputer, einschließlich der zugehörigen Festwert- und Schreib-Lese-Speicher, erforderlich.

Nach einem anderen bekannten System, nach dem die in der DE 41 37 124 A1 beschriebene Schaltung aufgebaut ist, werden die Eingangsdaten ebenfalls zwei Microcomputern parallel zugeführt, von denen jedoch nur einer die vollständige, aufwendige Signalverarbeitung ausführt. Der zweite Microcomputer dient vornehmlich zur Überwachung, weshalb die Eingangssignale nach Aufbereitung, Bildung von zeitlichen Ableitungen etc. mit Hilfe vereinfachter Regelalgorithmen und vereinfachter Regelphilosophie weiterverarbeitet werden können. Die vereinfachte Datenverarbeitung reicht zur Erzeugung von Signalen aus, die durch Vergleich mit den in dem aufwendigeren Microcomputer verarbeiteten Signalen Rückschlüsse auf den ordnungsgemäßen Betrieb des Systems zulassen. Durch die Verwendung eines Prüf-Microcomputers geringerer Leistungsfähigkeit läßt sich der Herstellungsaufwand im Vergleich zu einem System mit zwei vollständigen, aufwendigen Microcomputern gleicher Leistung reduzieren.

Aus der DE 43 41 082 A1 ist bereits ein Mikroprozessorsystem bekannt, das insbesondere für das Regelsystem einer blockiergeschützten Bremsanlage vorgesehen ist. Dieses bekannte System, das auf einem einzigen Chip untergebracht werden kann, enthält zwei Zentraleinheiten, in denen die Eingangsdaten parallel verarbeitet werden. Die Festwert- und die Schreib-Lese-Speicher, die an die beiden Zentraleinheiten angeschlossen sind, enthalten zusätzliche Speicherplätze für Prüfinformationen und umfassen jeweils einen Generator zur Erzeugung von Prüfinformationen. Die Ausgangssignale eines der beiden Zentraleinheiten werden zur Erzeugung -der Steuersignale weiterverarbeitet, während die andere als passive Zentraleinheit lediglich zur Überwachung der aktiven Zentraleinheit dient.

Bei den vorgenannten, bekannten Systemen wird also grundsätzlich die erforderliche Sicherheit durch Redundanz der Datenverarbeitung erreicht. Im ersten Fall (DE 32 34 637 C2) basiert das System auf die Verwendung von zwei Prozessoren mit identischer Software, was in Fachkreisen als symmetrische Redundanz bezeichnet wird. Im zweiten Fall (DE 41 37 124 A1) werden zwei Prozessoren mit unterschiedlicher Software verwendet (sog. asymmetrische Redundanz). Grundsätzlich ist es auch möglich, einen einzigen Prozessor zu verwerten, der auf Basis unterschiedlicher Algorithmen die Eingangsdaten verarbeitet, wobei dann zusätzliche Überprüfungsalgorithmen zum Feststellen eines fehlerfreien Arbeitens Anwendung finden.

Schließlich ist aus der DE 195 29 434 A1 (P7959) bereits ein System der eingangs genannten Art bekannt, das man als System mit Kernredundanz interpretieren könnte. Bei diesem bekannten Mikroprozessorsystem sind zwei synchron betriebene Zentraleinheiten auf einem oder auf mehreren Chips vorgesehen, die die gleichen Eingangsinformationen erhalten und das gleiche Programm abarbeiten. Die beiden Zentraleinheiten sind dabei über separate Bus-Systeme an die Festwert- und an die Schreib-Lese-Speicher sowie an Eingabe- und Ausgabeeinheiten angeschlossen. Die Bus-Systeme sind untereinander durch Treiberstufen bzw. Bypässe verbunden sind, die den beiden Zentraleinheiten ein gemeinsames Lesen und Abarbeiten der zur Verfügung stehenden Daten, einschließlich der Prüfdaten und Befehle ermöglichen. Das System ermöglicht eine Einsparung von Speicherplatz. Nur eine der beiden Zentraleinheiten ist (direkt) mit einem vollwertigen Festwert- und einem Schreib-Lese-Speicher verbunden, während die Speicherkapazität des zweiten Prozessors auf Speicherplätze für Prüfdaten (Paritätsüberwachung) in Verbindung mit einem Prüfdatengenerator beschränkt ist. Zugriff zu allen Daten besteht über die Bypässe. Dadurch sind beide Zentraleinheiten in der Lage, jeweils das vollständige Programm abzuarbeiten.

Alle vorgenannten Systeme beruhen grundsätzlich auf dem Vergleich redundant verarbeiteter Daten und der Erzeugung eines Fehlersignals, wenn Abweichungen auftreten. Beim Auftreten eines Fehlers oder Ausfall eines Systems kann dann die Regelung abgeschaltet werden. In keinem Fall ist eine Notlauffunktion, nämlich einer Fortsetzung der Regelung nach dem Auftreten des Fehlers, möglich. Eine solche Notlauffunktion wäre grundsätzlich nur durch Verdoppelung der redundanten Systeme in Verbindung mit einem Identifizieren und Abschalten der Fehlerquelle denkbar.

Der vorliegenden Erfindung liegt nun die Aufgabe zugrunde, ein Mikroprozessorsystem der eingangs genannten

Art mit höchstens geringem Mehraufwand derart auszugestalten, daß beim Auftreten eines Fehlers ohne Beeinträchtigung der Sicherheit eine Notlauffunktion möglich wird.

Es hat sich herausgestellt, daß diese Aufgabe durch das im Anspruch 1 beschriebene Mikroprozessorsystem gelöst werden kann. Die Besonderheit dieses Systems besteht darin, daß mindestens drei Zentraleinheiten mit den zugehörigen Bussystemen vorhanden sind, die durch redundante Peripherie-Einheiten zu mindestens zwei vollständigen Regelungssignalkreisen erweitert und derart zusammengeschaltet sind, daß bei Ausfall einer Zentraleinheit oder einer zugehörigen Komponente durch Majoritätsentscheid die fehlerhafte Zentraleinheit identifiziert wird und eine Notlauffunktion gewährleistet ist, wobei eine Ausgabe oder Erzeugung von Steuersignalen in Abhängigkeit von der fehlerhaften Zentraleinheit verhindert wird. Während der Notlauffunktion wird vorzugsweise eine redundante Datenverarbeitung und Vergleich der Datenverarbeitungsergebnisse auf Übereinstimmung aufrechterhalten und eine Nicht-Übereinstimmung der Datenverarbeitungsergebnisse signalisiert.

Die Erfindung geht also gewissermaßen von dem vorgenannten, aus der DE 195 29 434 A1 bekannten System aus, das im Prinzip aus einem vollständigen und einem unvollständigen Datenverarbeitungssystem besteht, und erweitert dieses System durch ein zusätzliches, vollständiges Datenverarbeitungssystem mit den zugehörigen Peripherie-Einheiten. Auf diese Weise entstehen zwei vollständige Regelungssignalkreise oder Regelungssignalverarbeitungssysteme, die zu einem notlauffähigen Gesamtsystem zusammengeschaltet sind, das auch bei Ausfall eines Prozessors bzw. einer Zentraleinheit eine Aufrechterhaltung der Regelung mit redundanter Datenverarbeitung und damit mit der geforderten hohen Sicherheit gewährleistet. Durch die erfindungsgemäße Zusammenschaltung der einzelnen Systeme oder Komponenten wird also auch bei Ausfall eines Prozessors die Redundanz der Datenverarbeitung aufrechterhalten.

Der Gesamtaufwand an Speicherplätzen, der wesentlich den Preis des Mikroprozessorsystems bestimmt, wird im Vergleich zu einer Verarbeitung in einem nicht redundanten System lediglich um wenig mehr als 100% erhöht, wobei die Aufteilung und Zuordnung der Speicherplätze zu den einzelnen Prozessoren in weiten Grenzen variabel ist; es muß lediglich sichergestellt sein, daß jeder einzelne Prozessor bzw. jede einzelne Prozessoreinheit das volle Programm abarbeiten kann und außerdem zu den Prüfdaten bzw. Redundanzdaten Zugriff hat. Im Vergleich zu einem nicht redundanten System wird eine verdoppelte Speicherkapazität, zuzüglich einiger Speicherplätze für die Redundanzdaten, benötigt.

Die erfindungsgemäße Ausgestaltung des Mikroprozessorsystems ermöglicht die Unterbringung aller oder der wesentlichen Komponenten, insbesondere sämtlicher Zentraleinheiten, Speicher, der Vergleicher und der Bypässe sowie ggf. auch der Eingabe- und Ausgabeeinheiten, auf einem einzigen Chip.

Nach einem Ausführungsbeispiel der Erfindung sind drei Zentraleinheiten mit je einem Bus-System vorgesehen sind, wobei für die Festwert- und für die Schreib-Lese-Speicher jeweils mindestens die doppelte Anzahl von Speicherplätzen im Vergleich zu den für ein nicht redundantes System benötigten Speicherplätzen zur Verfügung steht. Über die Bypässe sind alle Zentraleinheiten mit den Speicherplätzen in Schreib- und in Leserichtung und mit allen Eingabe- und Ausgabeeinheiten untereinander verbunden.

Die drei Zentraleinheiten bilden zusammen mit den Speichern, mit den Eingabe- und Ausgabeeinheiten und mit den Peripherie-Einheiten, einschließlich der Spannungsversorgung etc., insgesamt zwei vollständige und ein unvollständiges Datenverarbeitungssystem; die für einen vollständigen Programmablauf benötigten Speicherplätze sind allerdings auf jeweils zwei Datenverarbeitungssysteme aufgeteilt. Diese Datenverarbeitungssysteme umfassen vorteilhafterweise jeweils mindestens eine Zentraleinheit und ein Bus-System sowie Festwert- und Schreib-Lese-Speicher und/oder Redundanzinformationsspeicher, wobei die Speicherplätze derart auf die einzelnen Datenverarbeitungssysteme verteilt sind, daß beim Auftreten eines Fehlers und Übergang zur Notlauffunktion die intakten Systeme ausreichend Speicherplätze für die komplette Datenverarbeitung und für Redundanzinformationen enthalten und das komplette Programm abarbeiten.

Ein weiteres Ausführungsbeispiel nach der Erfindung besteht darin, daß zumindest die Zentraleinheiten mit den Bus-Systemen, die Speicher, die Bypass-Einheiten, die Eingabe- und Ausgabeeinheiten und einige oder alle Vergleicher auf einem gemeinsamen Chip angeordnet sind.

In den Unteransprüchen sind noch weitere vorteilhafte Ausführungsbeispiele beschrieben.

Aus der beigefügten Abbildung, welche in schematisch vereinfachter Darstellung die wesentlichen Komponenten eines Mikroprozessorsystems nach der Erfindung wiedergibt, und aus der nachfolgenden Beschreibung gehen weitere Einzelheiten der Erfindung hervor. Diese Abbildung dient zur Erläuterung des prinzipiellen Aufbaus und der Wirkungsweise eines Ausführungsbeispiels der Erfindung.

Die Abbildung bezieht sich auf ein Ein-Chip-Mikrocomputersystem, das drei synchron betriebene Prozessoren oder Zentraleinheiten **1**, **2**, **3**, die auch als Rechner- oder, wegen ihrer Funktion, als Prozessorkerne bezeichnet werden. Jedem Prozessor ist ein Bus-System **4**, **5**, **6** zugeordnet. Die Zentraleinheiten **1**, **2**, **3** sind an eine synchrone Taktversorgung cl (common clock), die redundant ausgelegt ist, angeschlossen.

Die Zentraleinheit **1** bzw. der Prozessorkern **1** ist durch einen Festwertspeicher **7** (ROM **1**), durch einen Schreib-Lese-Speicher **8** (RAM **1**), durch eine Eingabe- und Ausgabeeinheit **9** zu einem vollständigen Datenverarbeitungssystem oder Mikrocomputer MC1 ergänzt. Die notwendigen Peripheriekomponenten (Peripherie **1**) sind durch einen externen Block **10** symbolisiert. Zu den Peripheriekomponenten zählen die Spannungsversorgung, die Zuführung der Eingangssignale (z. B. der Sensorsignale bei einem KFZ-Regelungssystem) und die Aktuator- oder Ventilansteuerung etc. mit Hilfe der Ausgangsdaten oder -signale der Datenverarbeitungssysteme.

Ein zweites, unvollständiges Datenverarbeitungssystem oder Mikrocomputer MC2, in dem die Zentraleinheit **2** untergebracht ist, enthält im wiedergegebenen Ausführungsbeispiel lediglich Speicherplätze für Prüfdaten bzw. für die Redundanzfunktion. Symbolisch dargestellt sind im Inneren des Mikrocomputers MC2 Festwertspeicherplätze **12** für eine Paritätsüberwachung (Paritäts-ROM) und Speicherplätze **13** für die Redundanzdaten im Schreib-Lese-Bereich (Paritäts-ROM). Die zugehörigen Prüfdaten- oder Redundanzgeneratoren sind der besseren Übersichtlichkeit wegen nicht dargestellt.

Über das Bus-System **5** (BUS **2**) und über einen Bypass **14** sind BUS **1** (Bus-System **4**) und BUS **2** (Bus-System **5**) miteinander verbunden. Der Bypass **14** ermöglicht der Zentraleinheit **1** ein Lesen der in den Speicherplätzen **12**, **13** gespeicherten Paritätsdaten und gestattet einen Datenfluß von den Speichern **7**, **8** und dem Prozessorkern **1** des Mikrocomputers MC1 zu dem Mikrocomputer MC2, insbesondere zu der Zentraleinheit **2**. Auf diese Weise ist ein redundantes Abarbeiten des vollständigen Datenverarbeitungs-Programms durch beide Zentraleinheiten **1**, **2** gewährleistet.

Noch weitere Einzelheiten zu dem Aufbau und der Funktionsweise solcher Mikroprozessorsysteme sind der vorgenannten DE 195 29 434 A1 zu entnehmen.

Die Datenverarbeitungs-Ergebnisse beider Systeme MC1, MC2 bzw. Prozessoren **1, 2** werden, wie ebenfalls in der vorgenannten Schrift erläutert ist, mit Hilfe eines Vergleichers **15** auf Übereinstimmung überwacht; es ist ein unmittelbarer Vergleich der Ausgangssignale beider Prozessoren mit Hilfe eines Hardware-Vergleichers **15** vorgesehen.

Ein wesentliches Merkmal des Mikroprozessorsystems nach der Erfindung und des in der Abbildung dargestellten Ausführungsbeispiels besteht nun darin, daß das eben beschriebene, aus der DE 195 29 434 A1 bekannte System durch ein weiteres, vollständiges Datenverarbeitungssystem, nämlich durch einen Mikrocomputer MC3, der ebenfalls mit dem unvollständigen Mikrocomputer MC2 und auch mit dem Mikrocomputer MC1 zusammenwirkt, erweitert ist. Ein Teil der Funktionen des zusätzlichen Mikrocomputersystems (MC3), insbesondere das Speichern der Festwert- und der Schreib-Lese-Daten, kann allerdings auf das zweite Mikrocomputersystem MC2 und auch auf das erste System MC1 übertragen werden, weil das Gesamtsystem für die Gewährleistung der Redundanzfunktion insgesamt nur die doppelte Speicherkapazität, zuzüglich einiger Speicherplätze für die Redundanzinformation, im Vergleich zu einem nicht redundanten, das gleiche Programm abarbeitenden System benötigt. Die Speicherkapazität muß dabei auf die drei Datenverarbeitungssysteme MC1, MC2, MC3 derart verteilt werden, daß bei Ausfall eines Systems die verbleibenden Systeme einen ausreichenden Speicherplatz, nämlich mindestens 100% zuzüglich der Redundanzdaten, bieten. Im dargestellten Ausführungsbeispiel sind die beiden Mikrocomputersysteme MC1 und MC3 jeweils mit einer Speicherkapazität von 100% im Vergleich zu den für ein nicht redundantes System benötigten Speicherplätzen ausgerüstet, während sich im Mikrocomputersystem MC2 lediglich die wenigen Plätze für die Redundanzdaten befinden.

Das dritte Mikrocomputersystem MC3 ist mit dem (unvollständigen) Mikrocomputer MC2 ebenfalls durch einen Bypass bzw. eine Bypass-Einheit **16** verbunden. Dieser Bypass hat die gleiche Funktion wie der bereits eingehend beschriebene Bypass **14** und ermöglicht daher auch den Zentraleinheiten **2** und **3** die redundante Verarbeitung aller Eingangsdaten.

Das Mikroprozessorsystem MC3 enthält einen Festwertspeicher **17** (ROM **2**), einen Schreib-Lese-Speicher **18** (RAM **2**), eine Eingabe- und Ausgabeeinheit **19** und Peripherie-Komponenten **20** (Peripherie **2**). MC1 und MC3 sind im dargestellten Ausführungsbeispiel vollständige Mikrocomputer, für die allerdings, wie zuvor erläutert, eine reduzierte Speicherkapazität genügt.

Über die Bypässe **14, 16** ist ein Datenfluß in beiden Richtungen vom BUS **1** (Bus-System **4**) zum BUS **3** (Bus-System **6**) gegeben. Zur weiteren Erhöhung der Ausfallsicherheit könnte es eventuell sinnvoll sein, über einen zusätzlichen Bypass, der nicht dargestellt ist, eine direkte Verbindung zwischen diesen beiden Bus-Systemen **4, 6** (BUS **1** und BUS **3**) herzustellen.

Der Mikrocomputer MC3 besitzt hier den gleichen Aufbau und die gleichen Komponenten wie der Mikrocomputer MC1. Folglich sind bei dem erfindungsgemäßen Mikroprozessorsystem auch die Eingabe- und Ausgabeeinheiten **9, 19** und die Peripherie-Komponenten **20, 21**, zu denen die Spannungsversorgung, der Sensorsignaleingang und die Aktuatoransteuerung zählen, zweimal vorhanden.

Die Ausgangssignale oder Datenverarbeitungsergebnisse des dritten Mikrocomputers MC3 werden mit Hilfe eines Vergleichers **22** auf Übereinstimmung mit den Ergebnissen oder Ausgangssignalen des Mikrocomputers MC2 bzw. der Zentraleinheit **2** sowie in gleicher Weise mit Hilfe des Vergleichers **23** auf Übereinstimmung mit den Ergebnissen des MC1 bzw. der Zentraleinheit **1** überprüft. Dadurch ist nicht nur eine Fehlererkennung, sondern auch eine Identifizierung des Systems, in dem der Fehler liegt, möglich. In einer Identifizierungs-Stufe **24**, die vorzugsweise redundant ausgeführt und der die Ausgangssignale der Vergleicher **15, 22, 23** zugeleitet werden, wird durch eine Majoritätsentscheidung die Fehlerquelle erkannt und daraufhin das System auf eine Notlauffunktion umgeschaltet. Dies bedeutet, daß die Ausgabe von Steuersignalen in Abhängigkeit von den fehlerhaften Datenverarbeitungsergebnissen verhindert und statt dessen auf das intakte System umgeschaltet wird. Eine Verwertung der Datenverarbeitungsergebnisse während der Notlauffunktion ist deshalb auch bei sicherheitskritischen Regelungssystemen zulässig, weil auch bei Auftreten eines Fehlers weiterhin eine redundante Datenverarbeitung gewährleistet ist.

Das erfindungsgemäße System läßt sich mit vergleichsweise geringem Herstellungsaufwand realisieren. Im Prinzip genügt – im Vergleich zu dem bekannten System, das keinen Notlauf zuläßt – das Hinzufügen eines Prozessorkerns und die Erhöhung der Speicherkapazität auf das 1,5-fache. Eine klassische Lösung mit Notlauffunktion würde mindestens den dreifachen Speicheraufwand erfordern; dies ist ein entscheidender Vorteil, weil die Kosten des Gesamtsystems maßgeblich von der Größe der Arbeitsspeicher (Festwert- und Schreib-Lese-Speicher) bestimmt werden.

Der Aufwand für die Vergleicher **15, 22, 23**, die eine Identitätsüberwachung durchführen, ist minimal. Der Austausch von Signalen zwischen den einzelnen Mikrocomputern über die Bypässe erfordert keinen nennenswerten Aufwand. Programmtechnisch wird eine Software für ein scheinbares Einprozessorsystem realisiert; es werden keine Softwarestrukturen benötigt, die einen Austausch von Signalen zwischen den Mikrocomputern realisieren oder Signale auf Gleichheit oder Ähnlichkeit überprüfen.

Grundsätzlich ist es auch möglich, beim Auftreten eines internen Rechnerfehlers die Übernahme der Eingangsinformation und der Signalausgabe durch den fehlerfreien Kreis durchzuführen bzw. dem fehlerfreien Kreis zu übertragen. Dies führt zu weiteren Vereinfachungen und Systemfunktionen.

Patentansprüche

1. Mikroprozessorsystem für sicherheitskritische Regelungen, mit redundanter Datenverarbeitung, mit mehreren Zentraleinheiten (CPU's), die über separate Bus-Systeme mit Festwertspeichern und Schreib-Lesespeichern, die auch Speicherplätze für Prüfdaten enthalten, mit Eingabe- und Ausgabeeinheiten und mit Vergleichern, die die Ausgangsdaten oder Ausgangssignale der Zentraleinheiten auf Übereinstimmung überprüfen, verbunden sind und die das gleiche Programm abarbeiten, wobei die Zentraleinheiten über die Bus-Systeme miteinander kommunizieren und wobei die Bus-Systeme untereinander durch Bypässe verbunden sind, die den Zentraleinheiten ein gemeinsames Lesen und Abarbeiten der anstehenden Daten, einschließlich der Prüfdaten und Befehle, ermöglichen, **dadurch gekennzeichnet**, daß mindestens drei Zentraleinheiten (**1, 2, 3**) vorhanden sind, die durch redundante Periphere-Einheiten (**10, 20**) zu mindestens zwei vollständigen Regelungssignalkreisen erweitert und derart zusam-

mengeschaltet sind, daß bei Ausfall einer Zentraleinheit (**1, 2, 3**) und/oder zugehöriger Komponenten durch Majoritätsentscheidung in einer Identifizierungsstufe (**24**) die fehlerhafte Zentraleinheit identifizierbar und eine Notlauffunktion aufrechterhalten wird, wobei eine Ausgabe von Ausgangssignalen oder Steuersignalen unter Einschluß bzw. in Abhängigkeit von dem fehlerhaften Systems bzw. der fehlerhaften Zentraleinheit verhindert wird.

2. Mikroprozessorsystem nach Anspruch 1, dadurch gekennzeichnet, daß in der Notlauffunktion eine redundante Datenverarbeitung sowie Vergleich der Datenverarbeitungsergebnisse auf Übereinstimmung aufrechterhalten und eine Nicht-Übereinstimmung bzw. das Auftreten von Abweichungen zwischen den Datenverarbeitungsergebnissen oder Zwischenergebnissen signalisiert wird.

3. Mikroprozessorsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß drei Zentraleinheiten (**1, 2, 3**) mit je einem Bus-System (**4, 5, 6**) vorgesehen sind und daß für die Festwertspeicher (**7, 12, 17**) und für die Schreib-Lese-Speicher (**8, 13, 18**) jeweils mindestens die doppelte Kapazität, zuzüglich einiger Speicherplätze für die Redundanzdaten, im Vergleich zu der für ein nicht redundantes System benötigten Speicherkapazität zur Verfügung steht, wobei über die Bypässe (**14, 16**) eine Verbindung zwischen allen Zentraleinheiten (**1, 2, 3**) und den Speicherplätzen in Schreib- und Leserichtung und zu allen Eingabe- und Ausgabeeinheiten (**9, 10**) besteht.

4. Mikroprozessorsystem nach Anspruch 3, dadurch gekennzeichnet, daß die drei Zentraleinheiten (**1, 2, 3**) zusammen mit den Speichern (**7, 8, 12, 13, 17, 18**), mit den Eingabe- und Ausgabeeinheiten (**9, 10**) und mit den Peripherie-Komponenten (**10, 20**) insgesamt zwei vollständige und ein unvollständiges Datenverarbeitungssystem bilden.

5. Mikroprozessorsystem nach Anspruch 4, dadurch gekennzeichnet, daß die drei Datenverarbeitungssysteme jeweils mindestens eine Zentraleinheit (**1, 2, 3**) und ein Bus-System (**4, 5, 6**) sowie Festwert- und Schreib-Lese-Speicher (**7, 17; 8, 18**) und/oder Redundanzinformationsspeicher (**12, 13**) umfassen, wobei die Speicherplätze derart auf die einzelnen Datenverarbeitungssysteme verteilt sind, daß beim Auftreten eines Fehlers und Übergang zur Notlauffunktion die intakten Systeme ausreichend Speicherplätze für die komplette Datenverarbeitung und für die Redundanzinformationen enthalten und das komplette Programm abarbeiten.

6. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß den Vergleichern (**15, 22, 23**) jeweils die Datenverarbeitungsergebnisse bzw. Ausgangssignale von zwei Zentraleinheiten (**1, 2, 3**) zuführbar sind.

7. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß zumindest die Zentraleinheiten (**1, 2, 3**) mit den Bus-Systemen (**4, 5, 6**), die Speicher (**7, 8, 12, 13, 17, 18**), die Bypässe (**14, 16**), die Eingabe- und Ausgabeeinheiten (**9, 19**), Vergleicher (**15, 22, 23**) und Identifizierungsstufen (**24**) auf einem gemeinsamen Chip angeordnet sind.

8. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß dieses für mehrere oder eine Kombination von Kraftfahrzeug-Regelungssystemen, wie Brake-by-wire, ABS, ASR, ASMS etc., ausgelegt ist und daß die Notlauffunktion die Aufrechterhaltung des Betriebs aller Regelungssysteme erfaßt.

9. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß dieses für mehrere oder eine Kombination von Kraftfahrzeug-Regelungssystemen ausgelegt ist und daß die Notlauffunktion auf die Aufrechterhaltung des Betriebs ausgewählter Regelungsfunktionen, zum Beispiel besonders sicherheitskritischer Funktionen, beschränkt ist.

Hierzu 1 Seite(n) Zeichnungen

Int. Cl.[6]: G 06 F 11/14
Offenlegungstag: 22. Oktober 1998